

Exhibit 9

Exhibit 11: U.S. Patent No. 8,666,062

Claim 1	Exemplary Evidence of Infringement
<p>1[pre] A method of performing a finite field operation on elements of a finite field, the method comprising a processor:</p>	<p>Core Scientific, Inc. (hereinafter “Core”) performs a method for finite field operation on elements of a finite field, for example, during the transfer of Bitcoin to an address, which is a cryptographic operation, using a processor. <i>See, e.g.</i>:</p> <p>“The Company sells bitcoin it receives through mining.... Sales of digital assets awarded to the Company through its self-mining activities are classified as cash flows from operating activities. The Company does not have any off-balance sheet holdings of digital assets and does not safeguard digital assets for third parties.”</p> <p><i>See, e.g.</i>, Core Scientific., Inc., Quarterly report pursuant to Section 13 and 15(d), (Form 10-Q), at Note 1, filed Nov. 06, 2024, available at https://www.sec.gov/ix?doc=/Archives/edgar/data/1839341/000162828024045811/core-20240930.htm</p> <p>“Core Scientific, Inc. is a leader in digital infrastructure for bitcoin mining and high-performance computing. We operate dedicated, purpose-built facilities for digital asset mining and are a premier provider of digital infrastructure, software solutions and services to our third-party customers. We employ our own large fleet of computers (‘miners’) to earn digital assets for our own account and we provide hosting services for large bitcoin mining customers We derive the majority of our revenue from earning bitcoin for our own account (‘self-mining’).”</p> <p><i>See, e.g.</i>, Core Scientific., Inc., Quarterly report pursuant to Section 13 and 15(d), (Form 10-Q), at Note 1, filed Nov. 06, 2024, available at https://www.sec.gov/ix?doc=/Archives/edgar/data/1839341/000162828024045811/core-20240930.htm</p> <p>We finance our operations primarily through cash generated from operations, including the sale of self-mined bitcoin”</p> <p><i>See, e.g.</i>, Core Scientific, Inc. Form 10-K, at 67, filed Feb. 27, 2025, available at https://investors.corescientific.com/sec-filings/all-sec-filings/content/0001628280-25-008302/0001628280-25-008302.pdf</p>

Claim 1	Exemplary Evidence of Infringement
	<p><u>“Bitcoin signed messages have three parts, which are the Message, Address, and Signature.</u></p> <p>The message is the actual message text - all kinds of text is supported, but it is recommended to avoid using non-ASCII characters in the signature because they might be encoded in different character sets, preventing signature verification from succeeding.</p> <p>The address is a legacy, nested segwit, or native segwit address. Message signing from legacy addresses was added by Satoshi himself and therefore does not have a BIP. <u>Message signing from segwit addresses has been added by BIP137 ... The Signature is a base64-encoded ECDSA signature</u> that, when decoded, with fields described in the next section.” (Emphasis added)</p> <p><i>See, e.g.,</i> Message Signing, https://en.bitcoin.it/wiki/Message_signing.</p> <p>“This document describes a signature format for <u>signing messages with Bitcoin private keys.</u></p> <p>The specification is intended to describe the standard for signatures of messages that can be signed and verified between different clients that exist in the field today.” (Emphasis added)</p> <p><i>See, e.g.,</i> Bitcoin BIP137, https://github.com/bitcoin/bips/blob/master/bip-0137.mediawiki.</p> <p>In secp256k1, type secp256k1_fe consists of 5 or 10 machine words, depending on the machine’s word size: “field_5x52.h” applies to machines with 64bit word size and “field_10x32.h” applies to machines with 32bit word size. <i>See, e.g.:</i></p> <pre data-bbox="614 1090 1769 1411"> /** This field implementation represents the value as 5 uint64_t limbs in base * 2^52. */ typedef struct { /* A <u>field element f</u> represents the sum(i=0..4, f.n[i] << (i*52)) mod p, * where <u>p is the field modulus, 2^256 - 2^32 - 977.</u> * * The individual limbs f.n[i] can exceed 2^52; the field's magnitude roughly * corresponds to how much excess is allowed. The value * sum(i=0..4, f.n[i] << (i*52)) may exceed p, unless the field element is * normalized. */ uint64_t n[5]; } </pre>

Claim 1	Exemplary Evidence of Infringement
	<pre> /* * Magnitude m requires: * n[i] <= 2 * m * (2^52 - 1) for i=0..3 * n[4] <= 2 * m * (2^48 - 1) * * <u>Normalized requires:</u> * n[i] <= (2^52 - 1) for i=0..3 * sum(i=0..4, n[i] << (i*52)) < p * (together these imply n[4] <= 2^48 - 1) */ SECP256K1_FE_VERIFY_FIELDS } <u>secp256k1_fe</u>;</pre> <p><i>See, e.g.,</i> bitcoin/src/secp256k1/src/field_5x52.h</p> <p>“The points on the elliptic curve are the pairs of finite field elements.”</p> <p><i>See, e.g.,</i> '062 pat. at col. 1, lines 50-52.</p> <pre> /** <u>A group element in affine coordinates on the secp256k1 curve</u>, * or occasionally on an isomorphic curve of the form y^2 = x^3 + 7*t^6. * */ typedef struct { <u>secp256k1_fe</u> x; <u>secp256k1_fe</u> y; int infinity; /* whether this represents the point at infinity */ } secp256k1_ge;</pre> <p>...</p> <pre> /** A group element of the secp256k1 curve, in jacobian coordinates. * */ typedef struct { secp256k1_fe x; /* actual x: x/z^2 */ secp256k1_fe y; /* actual Y: y/z^3 */ secp256k1_fe z; int infinity; /* whether this represents the point at infinity */ } secp256k1_gej;</pre>

Claim 1	Exemplary Evidence of Infringement
	<p><i>See, e.g.</i>, bitcoin/src/secp256k1/src/group.h</p> <p>Core performs the method using a processor. <i>See, e.g.</i>:</p> <p>“The miners we operate are highly specialized computer servers built to use application-specific integrated circuit (“ASIC”) chips that are designed specifically to mine bitcoin. With miners we produce computing power, known as “hash rate,” with which we verify transactions on the Bitcoin blockchain. Bitcoin “mining” refers to the process of proposing and verifying transaction updates to the Bitcoin blockchain, which helps keep the Bitcoin network and its blockchain secure. Our bitcoin mining operation is focused on the generation of bitcoin by solving complex cryptographic algorithms to validate transactions on the Bitcoin network blockchain, which is commonly referred to as “mining.”</p> <p><i>See, e.g.</i>, Core Scientific, Inc. Form 10-K, at 6, filed Feb. 27, 2025, available at https://investors.corescientific.com/sec-filings/all-sec-filings/content/0001628280-25-008302/0001628280-25-008302.pdf</p>
1[a] obtaining a first set of instructions for performing the finite field operation on values representing the elements of the finite field;	<p>Core obtains a first set of instructions for performing the finite field operation on values representing the elements of the finite field.</p> <p>For example, Core’s miners obtain a first set of instructions (e.g., for executing <code>secp256k1_ge_set_gej</code>) for performing the finite field operation on values representing the elements of the finite field.</p> <p>For example, in <code>secp256k1</code>, type <code>secp256k1_fe</code> consists of 5 or 10 machine words, depending on the machine’s word size: “<code>field_5x52.h</code>” applies to machines with 64bit word size and “<code>field_10x32.h</code>” applies to machines with 32bit word size. <i>See, e.g.</i>:</p> <pre>/** This field implementation represents the value as 5 uint64_t limbs in base * 2^52. */ typedef struct { /* A <code>field_element_f</code> represents the sum(i=0..4, f.n[i] << (i*52)) mod p,</pre>

Claim 1	Exemplary Evidence of Infringement
	<pre> * where p is the field modulus, 2²⁵⁶ - 2³² - 977. * * The individual limbs f.n[i] can exceed 2⁵²; the field's magnitude roughly * corresponds to how much excess is allowed. The value * sum(i=0..4, f.n[i] << (i*52)) may exceed p, unless the field element is * normalized. */ uint64_t n[5]; /* * Magnitude m requires: * n[i] <= 2 * m * (2⁵² - 1) for i=0..3 * n[4] <= 2 * m * (2⁴⁸ - 1) * * Normalized requires: * n[i] <= (2⁵² - 1) for i=0..3 * sum(i=0..4, n[i] << (i*52)) <= p * (together these imply n[4] <= 2⁴⁸ - 1) */ SECP256K1_FE_VERIFY_FIELDS } secp256k1_fe; See, e.g., bitcoin/src/secp256k1/src/field_5x52.h “The points on the elliptic curve are the pairs of finite field elements.” See, e.g., '062 pat. at col. 1, lines 50-52. /** A group element in affine coordinates on the secp256k1 curve, * or occasionally on an isomorphic curve of the form y² = x³ + 7*t⁶. * ... */ typedef struct { secp256k1_fe x; secp256k1_fe y; int infinity; /* whether this represents the point at infinity */ } secp256k1_ge; ... /** A group element of the secp256k1 curve, in jacobian coordinates. * ... </pre>

Claim 1	Exemplary Evidence of Infringement
	<pre data-bbox="623 236 1615 432"> $\begin{array}{l} \text{*/} \\ \text{typedef struct \{ } \\ \text{ secp256k1_fe x; /* actual } x: x/z^2 /* \\ \text{ secp256k1_fe y; /* actual } Y: y/z^3 /* \\ \text{ secp256k1_fe z; } \\ \text{ int infinity; /* whether this represents the point at infinity */ } \\ \text{\} secp256k1_gej; } \end{array}$ </pre> <p data-bbox="707 481 1267 514"><i>See, e.g.,</i> bitcoin/src/secp256k1/src/group.h</p> <p data-bbox="612 554 1679 587">The result of <code>secp256k1_ge_set_gej</code> is unreduced and needs normalizing. <i>See, e.g.:</i></p> <pre data-bbox="612 620 1784 1011"> <math display="block">\begin{array}{l} \text{static int secp256k1_ecdsa_sig_sign(const secp256k1_ecmult_gen_context *ctx, } \\ \text{ secp256k1_scalar *sigr, secp256k1_scalar *sigs, const secp256k1_scalar *seckey, } \\ \text{ const secp256k1_scalar *message, const secp256k1_scalar *nonce, int *recid } \\ \text{\) \{ } \\ \text{ ...; secp256k1_ge r; ...; } \\ \text{ secp256k1_ecmult_gen(ctx, &rp, nonce); } \\ \text{ <u>secp256k1_ge_set_gej(&r, &rp);</u> } \\ \text{ secp256k1_fe_normalize(&r.x); } \\ \text{ secp256k1_fe_normalize(&r.y); } \\ \text{ secp256k1_fe_get_b32(b, &r.x); } \\ \text{ secp256k1_scalar_set_b32(sigr, b, &overflow); } \\ \text{ ...; if (...) \{ *recid = (...) \& secp256k1_fe_is_odd(&r.y); \} ...; } \\ \text{\} } \end{array}</math> </pre> <p data-bbox="707 1052 1341 1085"><i>See, e.g.,</i> bitcoin/src/secp256k1/src/ecdsa_impl.h</p> <p data-bbox="612 1126 1837 1272">The function <code>secp256k1_ge_set_gej</code> invokes <code>secp256k1_fe_mul</code>. That function invokes <code>secp256k1_fe_impl_mul</code>. That function invokes <code>secp256k1_fe_mul_inner</code>. Function <code>secp256k1_u128_accum_mul</code> is then invoked for each word of above finite field element <code>r</code> (typed <code>secp256k1_ge</code>). <i>See, e.g.:</i></p> <pre data-bbox="612 1297 1710 1387"> <math display="block">\begin{array}{l} \text{/* <u>Multiply two unsigned 64-bit values a and b</u> and write the result to r. */} \\ \text{static SECP256K1_INLINE void secp256k1_u128_mul(secp256k1_uint128 *r, } \\ \text{ uint64_t a, uint64_t b); } \end{array}</math> </pre>

Claim 1	Exemplary Evidence of Infringement
<p>1[b] executing the first set of instructions to generate an unreduced result completing the finite field operation;</p>	<p><i>See, e.g.</i>, bitcoin/src/secp256k1/src/int128.h</p> <p>Core executes the first set of instructions to generate an unreduced result completing the finite field operation.</p> <p>For example, Core' miners execute the first set of instructions (e.g., for executing <code>secp256k1_ge_set_gej</code>) to generate an unreduced result completing the finite field operation.</p> <p>For example, the result of <code>secp256k1_ge_set_gej</code> is unreduced and needs normalizing. <i>See, e.g.</i>:</p> <pre data-bbox="614 600 1776 980"> static int secp256k1_ecdsa_sig_sign(const secp256k1_ecmult_gen_context *ctx, secp256k1_scalar *sigr, secp256k1_scalar *sigs, const secp256k1_scalar *seckey, const secp256k1_scalar *message, const secp256k1_scalar *nonce, int *recid) { ...; secp256k1_ge r; ... secp256k1_ecmult_gen(ctx, &r, nonce); secp256k1_ge_set_gej(&r, &rp); secp256k1_fe_normalize(&r.x); secp256k1_fe_normalize(&r.y); secp256k1_fe_get_b32(b, &r.x); secp256k1_scalar_set_b32(sigr, b, &overflow); ...; if (...) { *recid = (...) secp256k1_fe_is_odd(&r.y); } ... } </pre> <p><i>See, e.g.</i>, bitcoin/src/secp256k1/src/ecdsa_impl.h</p> <p>The function <code>secp256k1_ge_set_gej</code> invokes <code>secp256k1_fe_mul</code>. That function invokes <code>secp256k1_fe_impl_mu1</code>. That function invokes <code>secp256k1_fe_mu1_inner</code>. Function <code>secp256k1_u128_accum_mu1</code> is then invoked for each word of above finite field element <code>r</code> (typed <code>secp256k1_ge</code>). <i>See, e.g.</i>:</p> <pre data-bbox="614 1274 1712 1356"> /* <u>Multiply two unsigned 64-bit values a and b</u> and write the result to r. */ static SECP256K1_INLINE void secp256k1_u128_mul(secp256k1_uint128 *r, <u>uint64_t</u> a, <u>uint64_t</u> b); </pre> <p><i>See, e.g.</i>, bitcoin/src/secp256k1/src/int128.h</p>

Claim 1	Exemplary Evidence of Infringement
<p>1[c] obtaining a second set of instructions for performing a modular reduction for a specific finite field;</p>	<p>Core obtains a second set of instructions for performing a modular reduction for a specific finite field.</p> <p>For example, Core's miners obtain a second set of instructions (e.g., for executing <code>secp256k1_fe_normalize</code>) for performing a modular reduction for a specific finite field.</p> <p>For example, the result of <code>secp256k1_ge_set_gej</code> is unreduced and needs normalizing. <i>See, e.g.:</i></p> <pre data-bbox="614 556 1776 948">static int secp256k1_ecdsa_sig_sign(const secp256k1_ecmult_gen_context *ctx, secp256k1_scalar *sigr, secp256k1_scalar *sigs, const secp256k1_scalar *seckey, const secp256k1_scalar *message, const secp256k1_scalar *nonce, int *recid) { ...; secp256k1_ge r; ...; secp256k1_ecmult_gen(ctx, &rp, nonce); secp256k1_ge_set_gej(&r, &rp); <u>secp256k1_fe_normalize(&r.x);</u> <u>secp256k1_fe_normalize(&r.y);</u> secp256k1_fe_get_b32(b, &<u>r.x</u>); secp256k1_scalar_set_b32(sigr, b, &overflow); ...; if (...) { *recid = (...) secp256k1_fe_is_odd(&<u>r.y</u>); } ...; }</pre> <p><i>See, e.g.,</i> bitcoin/src/secp256k1/src/ecdsa_impl.h</p> <p>The function <code>secp256k1_ge_set_gej</code> invokes <code>secp256k1_fe_mul</code>. That function invokes <code>secp256k1_fe_impl_mul</code>. That function invokes <code>secp256k1_fe_mul_inner</code>. Function <code>secp256k1_u128_accum_mul</code> is then invoked for each word of above finite field element <code>r</code> (typed <code>secp256k1_ge</code>). <i>See, e.g.:</i></p> <pre data-bbox="614 1225 1712 1315">/* Multiply two unsigned 64-bit values a and b and write the result to r. */ static SECP256K1_INLINE void secp256k1_u128_mul(secp256k1_uint128 *r, uint64_t a, uint64_t b);</pre> <p><i>See, e.g.,</i> bitcoin/src/secp256k1/src/int128.h</p>

Claim 1	Exemplary Evidence of Infringement
	<p>The function <code>secp256k1_fe_impl_normalize</code> ensures a field element does not exceed “field modulus, $2^{256} - 2^{32} - 977$”, per “<code>field_5x52.h</code>”. <i>See, e.g.:</i></p> <pre>SECP256K1_INLINE static void <u>secp256k1_fe_normalize</u>(secp256k1_fe *r) { ...; <u>secp256k1_fe_impl_normalize</u>(r); ... }</pre> <p><i>See, e.g.,</i> <code>bitcoin/src/secp256k1/src/field_impl.h</code></p> <pre>static void <u>secp256k1_fe_impl_normalize</u>(secp256k1_fe *r) { uint64_t t0 = r->n[0], t1 = r->n[1], t2 = r->n[2], t3 = r->n[3], t4 = r->n[4]; /* <u>Reduce</u> t4 at the start so there will be at most a single carry from the first pass */ ...; /* The first pass ensures the magnitude is 1, ... */ ...; /* ... except for a possible carry at bit 48 of t4 (i.e. bit 256 of the field element) */ ...; /* At most a single final <u>reduction is needed</u>; check if the value is >= the field characteristic */ ...; /* Apply the final reduction (for constant-time behaviour, we do it always) */ ...; /* If t4 didn't carry to bit 48 already, then it should have after any final reduction */ ...; /* Mask off the possible multiple of 2^{256} from the final reduction */ ...; r->n[0] = t0; r->n[1] = t1; r->n[2] = t2; r->n[3] = t3; r->n[4] = t4; }</pre> <p><i>See, e.g.,</i> <code>bitcoin/src/secp256k1/src/field_5x52_impl.h</code></p>
1[d] executing the second set of instructions on the unreduced result to generate a reduced result; and	<p>Core executes the second set of instructions on the unreduced result to generate a reduced result. For example, Core’s miners execute the second set of instructions (<i>e.g.</i>, for executing <code>secp256k1_fe_normalize</code>) on the unreduced result to generate a reduced result.</p> <p>For example, the result of <code>secp256k1_ge_set_gej</code> is unreduced and needs normalizing. <i>See, e.g.:</i></p> <pre>static int secp256k1_ecdsa_sig_sign(const secp256k1_ecmult_gen_context *ctx, secp256k1_scalar *sigr, secp256k1_scalar *sigs, const secp256k1_scalar *seckey, const secp256k1_scalar *message, const secp256k1_scalar *nonce, int *recid) {</pre>

Claim 1	Exemplary Evidence of Infringement
	<pre data-bbox="671 241 1622 491"> ...; secp256k1_ge r; ... secp256k1_ecmult_gen(ctx, &rp, nonce); secp256k1_ge_set_gej(&r, &rp); <u>secp256k1_fe_normalize</u>(&r.x); <u>secp256k1_fe_normalize</u>(&r.y); secp256k1_fe_get_b32(b, &<u>r.x</u>); secp256k1_scalar_set_b32(sig, b, &overflow); ...; if (...) { *recid = (...) secp256k1_fe_is_odd(&<u>r.y</u>); } ... } </pre> <p data-bbox="705 532 1339 567"><i>See, e.g.</i>, bitcoin/src/secp256k1/src/ecdsa_impl.h</p> <p data-bbox="614 608 1833 752">The function <code>secp256k1_ge_set_gej</code> invokes <code>secp256k1_fe_mul</code>. That function invokes <code>secp256k1_fe_impl_mul</code>. That function invokes <code>secp256k1_fe_mul_inner</code>. Function <code>secp256k1_u128_accum_mul</code> is then invoked for each word of above finite field element <code>r</code> (typed <code>secp256k1_ge</code>). <i>See, e.g.</i>:</p> <pre data-bbox="614 776 1706 866"> /* Multiply two unsigned 64-bit values a and b and write the result to r. */ static SECP256K1_INLINE void secp256k1_u128_mul(secp256k1_uint128 *r, uint64_t a, uint64_t b); </pre> <p data-bbox="705 907 1275 943"><i>See, e.g.</i>, bitcoin/src/secp256k1/src/int128.h</p> <p data-bbox="614 984 1786 1055">The function <code>secp256k1_fe_impl_normalize</code> ensures a field element does not exceed “field modulus, $2^{256} - 2^{32} - 977$”, per “<code>field_5x52.h</code>”. <i>See, e.g.</i>:</p> <pre data-bbox="614 1086 1622 1176"> SECP256K1_INLINE static void <u>secp256k1_fe_normalize</u>(secp256k1_fe *r) { ...; <u>secp256k1_fe_impl_normalize</u>(r); ... } </pre> <p data-bbox="705 1184 1326 1220"><i>See, e.g.</i>, bitcoin/src/secp256k1/src/field_impl.h</p> <pre data-bbox="614 1266 1833 1423"> static void <u>secp256k1_fe_impl_normalize</u>(secp256k1_fe *r) { uint64_t t0 = r->n[0], t1 = r->n[1], t2 = r->n[2], t3 = r->n[3], t4 = r->n[4]; /* <u>Reduce</u> t4 at the start so there will be at most a single carry from the first pass */ ... /* The first pass ensures the magnitude is 1, ... */ ... } </pre>

Claim 1	Exemplary Evidence of Infringement
	<pre data-bbox="671 230 1875 518"> /* ... except for a possible carry at bit 48 of t4 (i.e. bit 256 of the field element) */ ...; /* At most a single final reduction is needed; check if the value is >= the field characteristic */ ...; /* Apply the final reduction (for constant-time behaviour, we do it always) */ ...; /* If t4 didn't carry to bit 48 already, then it should have after any final reduction */ ...; /* Mask off the possible multiple of 2^256 from the final reduction */ ...; <u>r->n[0] = t0; r->n[1] = t1; r->n[2] = t2; r->n[3] = t3; r->n[4] = t4;</u> } </pre> <p data-bbox="713 535 1410 577"><i>See, e.g.,</i> bitcoin/src/secp256k1/src/field_5x52_impl.h</p>
<p>1[e] providing the reduced result as an output for use in a cryptographic operation.</p>	<p>Core provides the reduced result as an output for use in a cryptographic operation.</p> <p>For example, Core's miners provide the reduced result as an output for use in a cryptographic operation.</p> <p>For example, the result of <code>secp256k1_ge_set_gej</code> is unreduced and needs normalizing. <i>See, e.g.:</i></p> <pre data-bbox="620 838 1782 1220"> static int secp256k1_ecdsa_sig_sign(const secp256k1_ecmult_gen_context *ctx, secp256k1_scalar *sigr, secp256k1_scalar *sigs, const secp256k1_scalar *seckey, const secp256k1_scalar *message, const secp256k1_scalar *nonce, int *recid) { ...; secp256k1_ge r; ...; secp256k1_ecmult_gen(ctx, &rp, nonce); secp256k1_ge_set_gej(&r, &rp); secp256k1_fe_normalize(&r.x); secp256k1_fe_normalize(&r.y); <u>secp256k1_fe_get_b32(b, &r.x);</u> <u>secp256k1_scalar_set_b32(sigr, b, &overflow);</u> ...; if (...) { *recid = (...) secp256k1_fe_is_odd(&r.y); } ...; } </pre> <p data-bbox="713 1263 1347 1302"><i>See, e.g.,</i> bitcoin/src/secp256k1/src/ecdsa_impl.h</p> <p>The function <code>secp256k1_ge_set_gej</code> invokes <code>secp256k1_fe_mul</code>. That function invokes <code>secp256k1_fe_impl_mul</code>. That function invokes <code>secp256k1_fe_mul_inner</code>. Function</p>

Claim 1	Exemplary Evidence of Infringement
	<p>secp256k1_u128_accum_mul is then invoked for each word of above finite field element r (typed secp256k1_ge). <i>See, e.g.:</i></p> <pre data-bbox="614 328 1712 421">/* Multiply two unsigned 64-bit values a and b and write the result to r. */ static SECP256K1_INLINE void secp256k1_u128_mul(secp256k1_uint128 *r, uint64_t a, uint64_t b);</pre> <p><i>See, e.g.,</i> bitcoin/src/secp256k1/src/int128.h</p>